SANDIA REPORT

SAND2005-5411
Unlimited Release
Printed July, 2005

Generic Threat Profiles

David P. Duggan

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550

Sandia is a multiprogram laboratory operated by Sandia Corporation,
a Lockheed Martin Company, for the United States Department of Energy's
National Nuclear Security Administration under Contract DE-AC04-94AL85000.

Issued by Sandia National Laboratories, operated for the United States Department of Energy by Sandia Corporation.

Available to DOE and DOE contractors from
U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831

Telephone: (865) 576-8401
Facsimile: (865) 576-5728
E-Mail: reports@adonis.osti.gov
Online ordering: http://www.osti.gov/bridge

Available to the public from
U.S. Department of Commerce
National Technical Information Service
5285 Port Royal Rd.
Springfield, VA 22161

Telephone: (800) 553-6847
Facsimile: (703) 605-6900
E-Mail: orders@ntis.fedworld.gov
Online order: http://www.ntis.gov/help/ordermethods.asp?loc=7-4-0#online

SANDIA REPORT
SAND 2005-5411
Unlimited Release
Printed July 2005

Generic Threat Profiles

David P. Duggan
Sandia National Laboratories
PO Box 5800
Albuquerque, NM 87185

ABSTRACT

This report proposes a generic set of threat profiles to be used when there is a need to categorize threats against a cyber system. The six levels of threat are based upon characteristics that have been identified over the last seven years of work in cyber assessments. These categories are not associated with common names such as “nation-state”, “hacker” or others due to the overloaded nature of the names. Instead, each category is identified by the specific levels it achieves with respect to each characteristic.

Special thanks to the following individuals for their review and input to this document.

John Clem
Jennifer Depoy
Jason Stamp
Bill Young
Mary Young

Introduction

Threat profiles are a way to bin threat organizations of differing political, social, and motivation structures such that relevant characteristics may be utilized in identifying classes of attacks each might be able to carry out. Since all combinations of characteristics are not enumerated within this table, applying any organization to a category in the table may not be an exact fit. This should not be a problem since each level within a characteristic is just an approximation and should not be considered as hard fact. This threat table only includes threats that are malevolent in nature. Look for the partner table, Cyber Attack Classes, in a separate document.

Table 1 - Threat Characteristics

Category	Funding	Goal Intensity	Stealth	Physical Access	Cyber Skills	Implementation Time	Cyber Org Size
I	H	H	H	H	H	Decades/Years	Hundreds
II	H	H	H	M	M	Years	Tens of Tens
III	M	H	M	M	M	Months	Tens
IV	L	M	H	L	H	Months	Tens
V	L	M	M	L	M	Months	Ones
VI	L	L	L	L	L	Weeks	One

Category

There are six listed categories of threat in this table. Representative group names for each category have been intentionally left out to force comparison with the information listed within the table as opposed to some generalized understanding of the adversary group. Category I represents a threat that has the highest capability of all characteristic groups, while Category VI represents a threat that has the lowest capability of all characteristic groups. The categories in between have been created to provide enough separation within the characteristics to be useful.

There is no specific reason for using six categories. We didn't want to have too many as that would cause us to have too fine of granularity and might cause the table to grow even larger. Using less than six wouldn't allow for any differentiation between the different characteristics.

Funding

This characteristic has historically been one that is used when defining threat groups. Translating this to actual dollars is problematic since actual buying power of any currency fluctuates over time. Therefore, the meaning of each level has several orders of magnitude of difference. Representative levels within this characteristic look like:

- H – High funding level consisting of hundreds of thousands to many millions of dollars.
- M – Medium funding level consisting of thousands to hundreds of thousands of dollars.
- L – Low funding level consisting of zero to thousands of dollars.

Funding is a multiplier factor that can allow any other attribute to be enhanced to a greater level. However, by using funding to enhance one attribute, it might reduce another attribute. For instance, purchasing specific cyber skills might improve that category, but could elevate the level of detection possible since the organization is now using resources outside their own group and therefore might reduce stealth.

Goal Commitment Intensity

This characteristic is to be used to determine exactly how determined the threat group will be in achieving their goals or objectives. As we have seen throughout history, there are certain actions that we consider to be fanatical and are not realistically considered as a characteristic of a threat group. It is the intent to capture the possibility of this type of fanatical behavior as a characteristic of a threat.

Representative levels for this characteristic are:

- H – High level includes the possibility of expending a group-member life to achieve the goals of the organization. This level is highly motivated to achieve their goals, no matter what the obstacle.
- M – Medium level includes the possibility of having a group-member be caught or captured, possibly going to prison for their part.
- L – Low level is one where members of the threat group are not willing to place themselves at risk of being caught or captured.

Stealth

The definition of this characteristic is a little different than we have had in the past. Before, it was the intended level of stealth while achieving a goal, now it is defined as the required level of stealth necessary to achieve the goal. When the required level is not maintained, the goal will not be achieved. Representative levels are:

- H – High level is where loss of stealth prior to execution cannot be tolerated.
- M – Medium level is where loss of absolute stealth can be tolerated or where total stealth cannot be achieved due to other restrictions.
- L – Low stealth is where stealth prior to execution is not a requirement or where stealth is not considered as important to the threat group.

Physical Access

It helps to determine whether the group can place someone inside a protection zone to be able to tamper with a cyber device through physical means. The main intent of this characteristic is that a member of the threat group is able to gain physical access to some cyber resource for some portion of an attack. Access to certain design-level information is sometimes only available to someone with physical access to the actual system. The different levels are defined as:

- H – High level has the group able to gain physical access to cyber resources either by placing someone in the proper employment, turning an insider, or other means. This is most likely a long term commitment and a local presence.
- M – Medium level means the group is able to identify where physical access is needed and through some short-term method, such as blackmail, coercion, breaking and entering, is able to gain the required access. This requires a local presence.
- L – Low level means that the group does not have the means to physically access the cyber resource at any time they choose. It is most likely that they are not locally present to the resource.

Cyber Skills

This characteristic allows for the level of cyber skills that is contained within the organization. Consequent with raw skills is the ability to acquire training in the discipline. We do not include skills that are found outside the organization, or those that may be purchased, so the funding characteristic may influence this characteristic. Representative levels are defined as:

- H – High level is where there is plenty of high-level knowledge, such as PhD or expert-level understanding, and also medium and low skill level, such as system designers and coders. This level of cyber skills can maintain its own training program or R&D program in information technology and security.
- M – Medium level is where there is a good mix of cyber practitioners, but not a large contingent necessary for internal development and education. Some capacity for internal education exists, but not much for R&D.
- L – Low level is where there is minimal skill with information technology. The threat group has the ability to do coding and execution, but little else. There is no capacity for a training or R&D program.

Implementation Time

This characteristic shows the amount of total time that an organization can tolerate in planning, developing, and deploying a cyber attack. It includes time necessary for all steps up to the actual execution of an attack. A limiting factor in each level is the specific technology that is being examined. Time is shorter when dealing with technologies. Levels defined for this characteristic are:

- Decades/Years – Many, many years can be used to put things into place.
- Years – Several years can be taken to implement and to put into place.
- Months – Time necessary is on the order of months and may be due to factors such as technology turnover or attack components previously developed.
- Weeks – There is little time devoted to planning, development, and implementation of the attack.

Cyber Organization Size

This characteristic tries to allow for some dynamics within the size and social networking ability of the cyber portion of the membership of the threat group. The levels imply a structure of the group as well. Levels for this characteristic are defined as:

- Hundreds – There are hundreds of individuals working and communication together in the cyber arena.
- Tens of Tens – There are many small groups that communicate loosely between the groups. Limited information is moved between groups.
- Tens – Small workgroups that work independently.
- Ones – Individuals that work independently.